UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/604,434	07/21/2003	Carl L. Gilbert	LC0133 PUS	1433

7590 10/17/2005

Vincent C. Ilagan
ARTZ & ARTZ, P.C.
Suite 250
28333 Telegraph Road
Southfield, MI 48034

EXAMINER	
YANG, CLARA I	

ART UNIT	PAPER NUMBER
2635	

DATE MAILED: 10/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/604,434	GILBERT ET AL.	
	Examiner	Art Unit	
	Clara Yang	2635	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 July 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16,18 and 19* is/are rejected.

7)☒ Claim(s) *17 and 20* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 July 2004* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The abstract of the disclosure is objected to because the maximum length of 150 words has been exceeded. Correction is required. See MPEP § 608.01(b).

Allowable Subject Matter

2. Claims 17 and 20 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Objections

3. Claim 5 is objected to because of the following informalities:

- Claim 5 calls for "said common unique secret code", which lacks antecedent basis since claim 1 omits requiring a common unique secret code. The examiner considers claim 5 to depend on claim 4 instead of claim 1.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1, 4, 6, and 7 are rejected under 35 U.S.C. 102(b) as being anticipated by Simon et al. (US 5,937,065).

Referring to claims 1 and 6, Simon's method, as shown in Fig. 3, comprises the steps of: (a) remote control 12 (i.e., previously programmed key) transmitting its unique identification (ID) (i.e., key identification code) as an initial code to vehicle control circuit 14 at step 60 or encrypting and transmitting its unique ID at step 72 (see Figs. 1 and 3; and Col. 5, lines 3-19 and 34-64); (b) control circuit 14 (i.e., electronic control module) waking up and executing an authentication protocol by verifying that remote control 12 sent the proper initial code at step 64, generating a challenge number at step 66, transmitting the challenge number at step 68, deriving an expected answer at step 74, comparing the answer received from remote control 12 and the expected answer at step 76, and determining if the received ID is valid at step 80 (see Col. 5, lines 20-33 and Col. 6, lines 13-43); and (c) control circuit 14 storing a list of valid remote control IDs (i.e., storing key identification codes in an active status) (i.e., see Col. 6, lines 36-43). Regarding the last limitation of claim 6, Simon's method also includes the step of (d) remote control 12 generating and transmitting a valid response at steps 70 and 72, wherein the valid response includes an answer (i.e., a key password), remote control 12's unique ID (if the ID as not transmitted at step 62), and switch indication (see Col. 5, lines 49-64 and Col. 6, lines 1-12). Per Simon, control circuit 14 temporarily stores the answer, unique ID, and switch indication at step 73 (see Col. 6, lines 8-12).

Regarding claims 4 and 7, referring again to Fig. 3, when control circuit 14 determines that remote control 12's answer matches the expected answer derived by control circuit 14 at step 76 (see Col. 6, lines 13-28), control circuit 14 indirectly determines that it shares a common seed number (i.e., unique secret code) with remote control 12. Simon teaches that remote

control 12 and control circuit 14 both use the same seed number with the same encryption algorithm to encrypt a challenge number (see Col. 5, lines 46-51 and Col. 6, lines 13-28).

6. Claims 1-7 and 12-15 are rejected under 35 U.S.C. 102(b) as being anticipated by Liden et al. (US 2001/0028298).

Referring to claims 1 and 6, Liden teaches a key 101 (i.e., previously programmed key) and lock 20 (i.e., electronic control module of a security system), as shown in Figs. 1 and 2, and a method that includes the steps of: (a) key 101 transmitting its key code, which contains its unique identity (UID) (i.e., key identification code), to lock 20 via key contact 101c and lock contact 20c (see Sections [0058], [0062], [0087]-[0096], [0101], and [0112]-[0113]); (b) key 101 and lock 20 executing an authentication protocol for key 101 (see Sections [0075], [0101], [0109], and [0112]-[0114]); and (c) lock 20 storing a list of authorized keys called the "A-list" comprising the public key ID (PKID) and secret key ID (SKID) of the authorized keys (i.e., storing key identification codes in an active status) (see Sections [0112]-[0113]). Regarding the last limitation of claim 6, Liden teaches that key 101's key code also includes a master key identification (MKS) (i.e., a key password), wherein lock 20 accepts a key 101 only if they have the same MKS code (see Sections [0087]-[0096] and [0101]); hence Liden's key 101 transmits its UID and MKS when it transmits its PKID, which is a valid response if key 101's PKID is not on the non-authorized keys list called the "NA-list".

Regarding claims 2 and 12, Liden discloses lock 20 comparing key 101's PKID to those listed on the NA-list, wherein the NA-list is stored within lock 20 (see Sections [0112]-[0113]).

Regarding claims 3 and 13, Liden further teaches the step of lock 20 determining that the PKID is identical to at least one PKID on the NA-list stored in lock 20 (see Sections [0112]-[0113]).

Regarding claims 4 and 7, Liden discloses that lock 20 and key 101 both include a data encryption standard (DES) key (i.e., a common unique secret code) that is used by key 101 and lock 20 to encrypt and decrypt data (see Sections [0084], [0094], and [0109]); thus lock 20 must determine that its DES key and key 101's DES key are the same if lock 20 is able to match key 101's PKID and SKID with those on the A-list (or match key 101's PKID with a PKID on the NA-list) since a successful match indicates that both DES keys are identical.

Regarding claims 5 and 14, Liden teaches that programming boxes 106 and/or C-keys are used for programming lock 20 and for adding and deleting items in the A-list and the NA-list of lock 20 (see Sections [0028]-[0029], [0036], [0175], [0182], and [0186]). Liden adds that D-keys (with D-software) and M-keys (with M-software) are used to download (i.e., transmit) necessary secret information (e.g., the DES key) to lock 20 (see Sections [0046]-[0047] and [0201]). Liden's D-software and M-software maintain a database of encryption keys, etc. (see Section [0029]). Therefore, Liden teaches transmitting at least one key code and a common unique secret code from a supplementary database to lock 20.

Regarding claim 15, Liden teaches the steps of: (a) comparing a key's PKID to at least one PKID on the NA-list (i.e., one disabled identification code stored in the electronic control module) (see Section [0113]); and (b) comparing the key's master key identification (MKS) to lock 20's MKS (see Section [0077]-[0086] and [0101)], which is a module password.

7. Claims 1-7 and 12-16 are rejected under 35 U.S.C. 102(e) as being anticipated by Kuenzi et al. (US 2004/0025039).

Referring to claims 1 and 6, Kuenzi's method, as shown in Figs. 4B-4C, comprises the steps of: (a) a key device (i.e., a previously programmed key) sending its personal identification number (PIN) (i.e., identification code), its first and second authorization tokens, and its serial

number (also an identification code) to a lock box (i.e., electronic control module) in step 470 (see Sections [0043], [0131], [0137], [0147], [0149], [0198], [0201], and [0205]); (b) the key device and lock box executing an authentication protocol for the key device in steps 480-570 (see Sections [0206]-[0212]); and (c) the lock box storing a list of valid PINs (i.e., storing key identification codes in an active status) (see Sections [0043], [0129], and [0137]). As for the remaining limitation of claim 6, Kuenzi teaches that a key device's system code (i.e., key password) must match the one stored in the lock box in order to be authorized by the lock box (see Section [0123]); thus Kuenzi's method comprises the steps of (d) the key device transmitting a valid response signal that includes the key password.

Regarding claims 2 and 12, Kuenzi's method comprises the step of the lock box comparing a key device's serial number to those stored on a lockout list (see Section [0130]).

Regarding claims 3 and 13, Kuenzi's method comprises the step of the lock box determining that a key device's serial number is identical to one of the serial numbers on the lockout list (i.e., one of the disabled identification codes) (see Section [0131]).

Regarding claims 4 and 7, Kuenzi teaches the step of the lock box determining that the encryption key stored at address A3 in the key device's memory and K_{PIN} (i.e., a common unique secret code) stored at the lock box are identical when the key device's response to the lock box's challenge matches the response generated by the lock box (see Figs. 4B and 4C, steps 520-550; and Sections [0210]-[0212]).

Regarding claims 5 and 14, Kuenzi discloses that the key device transmits at least its PIN, first and second authorization tokens, and serial number to the lock box, wherein the second token includes K_{PIN}, which is stored in the key device's memory (i.e., a supplementary database to the lock box) (see Sections [0200]-[0205] and [0123]).

Regarding claim 15, Kuenzi's method comprises the steps of: (a) the lock box comparing a key device's serial number to those stored on a lockout list (see Section [0130]), as explained in the previous rejection of claim 2; and (b) the lock box comparing the key device's system code (i.e., key password) to its own system code (i.e., module password) (see Section [0123]).

Referring to claim 16, Kuenzi's key device (i.e., primary electronic control module for controlling access to key container 258 via a dual-acting solenoid 712 as explained in Sections [0028], [0133]-0135], [0223], and [0225]-[0231]) comprises, a shown in Fig. 2, the following: (a) IR transceiver 260, (b) memory 262, and (c) central processing unit (CPU) 250 coupled to IR transceiver 260 and memory 262 (see Sections [0028], [0123], and [0203]-[0213]). Kuenzi's system also includes a key device (i.e., a previously programmed key), as shown in Fig. 2, that has: (a) memory 202 (i.e., electronic circuitry) with authorization tokens (i.e., key identification codes) stored therein (see Sections [0027], [0037]-[0039], [0198], [0201], and [0202]); and (b) IR transceiver 208 for transmitting the authorization tokens to the lock box (see Sections [0029] and [0205]). Kuenzi teaches that the key device and the lock box are able to communicate via radio frequency (RF) communication (see Sections [0030] and [0203]) rather than IR communication; hence, Kuenzi's lock box must comprise an antenna coupled to CPU 250, and the key device must also have an antenna for transmitting its authorization tokens when RF communication is used. Kuenzi teaches that the lock box's memory 262 stores: (a) key devices that are not allowed to access the lock box in a lockout list (see Section [0131]); and (b) the lock box's system code (i.e., module password) (see Section [0123]). Kuenzi's lock box is also able to temporarily store a key device's K_{PIN} (i.e., unique secret code) (see Sections [0207] and [0211]). Per Kuenzi, the lock box's CPU executes the authentication protocol shown in Figs. 4B and 4C, wherein the

authentication protocol further includes comparing a key device's serial number (i.e., key identification code) to those on the lockout list (see Sections [0131] and [0203]-[0213]).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

10. Claims 2, 3, 12, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Simon et al. (US 5,937,065) as applied to claims 1 and 6 above, and further in view of Liden et al. (US 2001/0028298).

Regarding claims 2, 3, 12 (which calls for the same limitation as claim 2), and 13 (which calls for the same limitation as claim 3), Simon's control circuit 14 stores a list containing a valid ID for each remote control 12 that is authorized to operate the vehicle, compares a unique ID received from remote control 12 to those on the list, and determines that the received unique ID is identical to one of the IDs on the list (see Col. 6, lines 36-43). Simon, however, fails to teach:

(1) control circuit 14 comparing the received unique ID to at least one disabled ID stored in control circuit 14 (as called for in claims 2 and 12); and (2) control circuit 14 determining that the received unique ID is identical to at least one disabled ID stored within control circuit 14 (as called for in claims 3 and 13).

Liden's system and method, as explained in the 35 USC 102(b) rejection of claims 1-7 and 12-15, are reasonably pertinent to the particular problem with which the applicant was concerned; hence Liden's teaching is analogous art. As explained in the 35 USC 102(b) rejection of claims 1 and 6, Liden's lock 20 (i.e., electronic control module) stores an A-list comprising the public key ID (PKID) and secret key ID (SKID) of each authorized keys as well as a list of non-authorized keys (NA-list) (see Sections [0112]-[0113]). The NA-list comprises only the PKID of non-authorized keys (see Section [0113]).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Simon's system and method as taught by Liden because having a list of unique ID for each unauthorized remote control 12 in addition to a list of valid unique IDs enables a user to easily deactivate and reactivate remote control 12s by simply adding the unique ID of each remote control 12 to a list of unauthorized unique IDs when a remote control 12 is to be deactivated and by removing the unique ID from the list of unauthorized unique IDs when a remote control 12 is to be reactivated (see Liden, Sections [0164]-[0167]).

11. Claims 8-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Simon et al. (US 5,937,065) as applied to claim 7 above, and further in view of Alrabady et al. (US 6,658,328).

Regarding claims 8-11, Simon's method as shown in Fig. 3, comprises: (a) control circuit 14 generating a challenge number at step 66, wherein the challenge number is randomly

generated (see Col. 5, lines 28-31); (b) control circuit 14 transmitting the challenge number to remote control 12 at step 68 (see Col. 5, lines 31-33), as called for in the second limitation of claim 8; (c) control circuit 14 comparing remote control 12's answer (i.e., key password) to the answer derived by and temporarily stored at control circuit 14 at step 76 (see Col. 6, lines 13-30), as called for in claim 10; and (d) control circuit 14 determining that remote control 12's answer is identical to control circuit 14's derived answer (i.e., module password) at step 78 (see Col. 6, lines 30-41), as called for in claim 11. Simon's method, however, lacks the steps of: (1) control circuit 14 transmitting encrypted predetermined data, as called for in the first limitation of claim 8, along with the challenge number; (2) remote control 12 comparing the predetermined data to a key authentication data stored within remote control 12, as called for in the last limitation of claim 8; and (3) remote control 12 determining that the predetermined data is identical to the key authentication data, as called for in claim 9.

In an analogous art, Alrabady teaches an authentication method, as shown in Figs. 2 and 3, comprising the steps of: (a) vehicle controller 18 (i.e., electronic control module) generating a random number and retrieving an ID code (i.e., predetermined data) at step 306 (see Col. 5, lines 66-67 and Col. 6, lines 1-3); (b) controller 18 encrypting a portion of the random number and a portion of the ID code at step 308 (see Col. 6, lines 3-6), as called for in claim 8; (c) controller 18 assembling a challenge signal, which includes the encrypted and non-encrypted portions of the random number and ID code and transmitting the challenge signal to portable transceiver 16 (i.e., previously programmed key) at step 310 (see Col. 6, lines 12-35), as called for in claim 8; (d) portable transceiver 16 receiving the challenge signal at step 206, comparing the non-encrypted portion of the ID code with a corresponding portion of a stored reference code (i.e., key authentication data) at step 210, decrypting the random number and the ID code if the

non-encrypted portion of the ID code matches the reference code's corresponding portion at step 212, and comparing the decrypted ID code with the reference code's corresponding portion at step 214 (see Col. 6, lines 51-67 and Col. 7, lines 1-31), as called for in claim 8; and (e) portable transceiver 16 determining that the received ID code is identical to the reference ID code at steps 210 and 214 (see Col. 6, lines 60-67 and Col. 7, lines 1-12 and 18-31), as called for in claim 9.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Simon's system and method as taught by Alrabady because the steps first comparing non-encrypted portion of the ID code and then comparing the encrypted portion of the ID code only if the non-encrypted portion is identical to a corresponding portion of the reference ID code decrease remote control 12's power consumption if the non-encrypted portion of the ID code fails to match the reference ID code's corresponding portion since fewer than all of the ID code bits are compared (see Alrabady, Col. 8, lines 57-67 and Col. 9, lines 1-6). In addition, the steps of control circuit 14 transmitting an ID code and remote control 12 verifying the received ID code ensure that remote control 12 only responds to a challenge signal transmitted by control circuit 14 of the correct vehicle.

12. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Simon et al. (US 5,937,065) in view of Liden et al. (US 2001/0028298).

Referring to claim 16, Simon's security system, as shown in Fig. 1, includes: (a) control circuit 14 (i.e., primary electronic control module) comprised of antenna 32 and microcomputer 16, wherein microcomputer 16 has an internal microprocessor and memory and is coupled to antenna 32 via radio frequency (RF) transceiver 30 (see Col. 3, lines 48-54 and Col. 4, lines 6-14); (b) remote control 12 (i.e., previously programmed key) comprised of EEPROM 48 (i.e., electronic circuitry), which stores a unique ID code for the remote control, and transceiver 40 for

transmitting the unique ID to control circuit 14's antenna 32 (see Col. 4, lines 16-36 and Col. 5, lines 13-19 and 56-60); (c) antenna 32 receiving the unique ID and forwarding the unique ID to microcomputer 16 (see Col. 4, lines 6-14 and Col. 6, lines 8-12); (d) microcomputer 16's memory storing a seed number (i.e., unique secret code) (see Col. 3, lines 48-54 and Col. 6, lines 13-28); and (e) microcomputer 16 executing an authentication protocol for remote control 12 by comparing remote control 12's unique ID with those on a list of valid remote control IDs (see Col. 5, lines 13-16, 26-28, and 56-64; and Col. 6, lines 8-43). Simon's control circuit 14 does not store a list of disabled remote control IDs and is therefore unable to compare a received unique ID to those on the list of disabled remote control IDs.

In an analogous art, as explained in the previous 35 USC 103(a) rejection of claims 2, 3, 12, and 13, Liden's lock 20 (i.e., electronic control module) stores an A-list comprising the PKID and SKID of each authorized keys as well as a list of non-authorized keys (NA-list) (see Sections [0112]-[0113]). The NA-list comprises only the PKID of non-authorized keys (see Section [0113]).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Simon's system and method as taught by Liden because having a list of unique ID for each unauthorized remote control 12 in addition to a list of valid unique IDs enables a user to easily deactivate and reactivate remote control 12s by simply adding the unique ID of each remote control 12 to a list of unauthorized unique IDs when a remote control 12 is to be deactivated and by removing the unique ID from the list of unauthorized unique IDs when a remote control 12 is to be reactivated (see Liden, Sections [0164]-[0167]).

13. Claims 18 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Simon et al. (US 5,937,065) in view of Liden et al. (US 2001/0028298) as applied to claim 16 above, and further in view of Alrabady et al. (US 6,658,328).

Regarding claims 18 and 19, Simon, as modified by Liden, teaches that control circuit 14's microcomputer 16 applies an encryption algorithm and a seed number (i.e., unique secret code) for deriving an expected answer (i.e., module password) to the challenge number (see Col. 6, lines 13-28). Microcomputer 16 of Simon and Liden temporarily stores remote control 12's unique ID (i.e., key identification code) when remote control 12's answer (i.e., key password) exactly matches microcomputer 16's derived answer (i.e., module password) in order for microcomputer 16 to determine if the unique ID is valid (see Col. 6, lines 8-43), as called for in claim 19. Because microcomputer 16 only compares the received unique ID to those on the list of valid IDs (see Col. 6, lines 30-41), the received ID is stored for comparison by microcomputer 16 when remote control 12's response signal is valid, as called for in claim 18. Simon and Liden, though, omit teaching that microcomputer 16 encrypts a signal with the encryption algorithm and seed number, as called for in claims 18 and 19.

In an analogous art, as explained in the 35 USC 103(a) rejection of claims 8-11, Alrabady teaches an authentication method, as shown in Figs. 2 and 3, comprising the steps of: (a) vehicle controller 18 (i.e., electronic control module) generating a random number and retrieving an identification (ID) code (i.e., predetermined data) at step 306 (see Col. 5, lines 66-67 and Col. 6, lines 1-3); (b) controller 18 encrypting a portion of the random number and a portion of the ID code at step 308 (see Col. 6, lines 3-6); and (c) controller 18 assembling a challenge signal, which includes the encrypted and non-encrypted portions of the random number and ID code and

transmitting the challenge signal to portable transceiver 16 (i.e., previously programmed key) at step 310 (see Col. 6, lines 12-35).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Simon and Liden's system and method as taught by Alrabady because the steps of control circuit 14 transmitting a signal containing non-encrypted and encrypted portions of an ID code and remote control 12 verifying the received ID code ensure that remote control 12 only responds to a challenge signal transmitted by control circuit 14 of the correct vehicle.

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Pogue, Jr. et al. (US 5,144,667) teach a vehicle security system comprising a remote unit and a vehicle base unit that communicate via a radio link secured by an exchange of encrypted signals.
- Thompson, Jr. et al. (US 5,978,483) teach a secure remote keyless entry (RKE) system wherein transmitter 12 uses a unique encryption algorithm to generate a multibit message having a pseudorandom number, a key code, and the transmitter ID encrypted within.
- Davies (US 2003/0149666) teaches a device authentication system wherein a fob responds to an encrypted challenge signal transmitted from a vehicle by decrypting the signal using a private key, determining if the challenge is valid, and transmitting a response.
- Janssen et al. (US 6,617,961) teach a vehicle security system a vehicle controller transmits an encrypted data packet containing its ID and a fob that receives the encrypted signal, decrypts the signal, and compares the ID with a stored reference ID. If the received ID and the reference ID are identical, the fob then transmits a response data packet.

⌘⌘⌘

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Clara Yang whose telephone number is (571) 272-3062. The examiner can normally be reached on 8:30 AM - 7:00 PM, Monday - Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael Horabik can be reached on (571) 272-3068. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CY
13 October 2005